Why Advanced Security Is an Essential Element of an Effective SD-WAN Solution

Table of Contents

Executive Summary

The traditional wide-area networks (WANs) currently in place at most organizations can no longer support the traffic demands of digital transformation and high volumes of off-site workers. Modernizing WAN infrastructure has become unavoidable.[1] Many companies are choosing software-defined WAN (SD-WAN) solutions as a replacement. But the majority of SD-WAN products on the market today lack full and robust solution capabilities—especially in terms of built-in security.

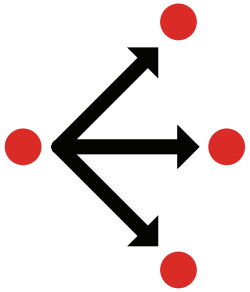
For successful WAN transformation, organizations need an approach that integrates sophisticated networking and security capabilities in a single secure SD-WAN solution. A unified platform for SD-WAN can ensure consistent protection and simplify network infrastructure, while enabling granular policy-based controls based on a zero-trust access approach.

Security Is a Missing Link in WAN Transformation

The combination of new digital tools, cloud adoption, and large numbers of teleworkers requiring remote access has made it impossible for traditional WAN architectures to handle traffic demands at the network edge. Traditional WANs use expensive multiprotocol label switching (MPLS) connections as well as centralized security performed by backhauling traffic through the corporate data center. This dependent structure creates bottlenecks that degrade end-user performance.

As a more modern alternative, many organizations are choosing SD-WAN for their distributed network performance needs. SD-WAN offers significant advantages over MPLS for both bandwidth and cost by dynamically selecting from a variety of commodity internet connections (e.g., LTE, DSL, 4G/5G, Ethernet). But one significant change that comes with SD-WAN is that these direct connections to cloud and internet resources bypass the hub-and-spoke security of traditional architectures. This wide-open exposure to threats requires robust security—and many of today's SD-WAN networking solutions have little to no built-in security.

This leads many organizations to add disparate tools to address the shortcomings of their specialized SD-WAN networking device. This siloed approach increases both capital expenditures and operational costs while increasing infrastructural complexity and creating potential gaps for cyberattacks to slip past defenses. As threats continue to grow in number and sophistication, integrated security is increasingly essential for any WAN transformation project.



MPLS connectivity cannot meet the radical change in network demands caused by digital transformation and an increasingly distributed workforce. SD-WAN can.[2]

How a Secure SD-WAN Solution Can Help

Successful WAN transformation needs to provide a consistent user experience while ensuring effective security and efficient operations at scale. To avoid the pitfalls of a piecemeal approach to SD-WAN, organizations should look for a solution that combines robust capabilities for both networking and security functions. This unified approach should offer a solution that provides consistent protection, greater operational efficiency, and advanced features that anticipate evolving network demands over time.

Consistent Protection

An integrated secure SD-WAN solution should provide consistent protection that eliminates both security and performance tradeoffs. It should offer robust security capabilities that are built-in—such as secure sockets layer (SSL)/transport layer security (TLS) encrypted traffic inspection. Most SD-WAN solutions do not offer adequate inspection—even though SSL/TLS encryption now comprises about 85% of network traffic.[3] Some solutions that claim to offer decryption cannot truly inspect all traffic because performance is drastically impacted. Others do not offer TLS 1.3 decryption, letting anything hidden in that traffic into the network. If all traffic is not inspected, malware and other threats slip right through perimeter defenses.

Critical application prioritization. Connectivity alone isn't enough, especially with widespread remote work. An effective SD-WAN solution needs to identify a broad set of applications to meet all use cases. Advanced self-healing WAN automation capabilities can help provide a consistent user experience on any transport for any user. Many SD-WAN solutions are unable to support either a large number of application signatures or application performance optimization. This causes inconsistent user experience and/or support for only limited use cases.

Reduced attack surface. A standalone SD-WAN device is simply a connectivity offering that provides an open conduit for threats to attack the network. Protecting these devices with standalone security solutions has distinct limitations because they cannot adapt to dynamic connectivity environments. To protect modern WAN environments, advanced security needs to be embedded into each SD-WAN device. This allows home users, branch office users, and the data center to use a common set of security policies and enforcement criteria. Networking, connectivity, and security functions become so tightly integrated that they can operate as a single, unified solution, even under dynamic conditions.

Comprehensive analytics and reporting. A secure SD-WAN solution needs to help organizations gain visibility into network and application performance (both real-time and historical statistics). That includes enhanced analytics as well as enhanced compliance. A single management console for both networking and security with rich SD-WAN analytics can help organizations fine-tune business and security policies to improve quality of experience for all users.

In the last year, ransomware attacks have increased 150% and the amount paid by victims has risen 300%.[4]

Greater Infrastructure Simplicity

An SD-WAN solution that seamlessly scales and integrates security and networking simplifies the distributed network's architectural design, management, and operation. It helps organizations automate remote site deployments, while consolidating networking and security infrastructure. This results in improved mean time to remediation (MTTR) of issues and better return on investment (ROI).

Integrated security and networking. A platform-based approach to SD-WAN includes advanced networking and security capabilities that are explicitly designed to interoperate as a unified system—ideally running on the same operating system and managed via a single pane of glass. This ensures that transactions are all seen and inspected, and any threats or anomalous behaviors are shared between every product in the ecosystem for maximum protection. A comprehensive secure SD-WAN platform can also consolidate a range of point products—including routers, firewalls, and access proxy for zero-trust network access (ZTNA)—into a single product, simplifying architecture and reducing capital investment costs.

Simplified management and orchestration. Centralized secure SD-WAN management ensures that new services and policies are application-focused. In addition, connectivity and security configurations and policy changes can be seamlessly propagated throughout the extended WAN. This reduces error and eliminates the need to configure or manage each device or service individually. Centralized secure SD-WAN also provides rich analytics showing historic and real-time application performance, allowing teams to quickly troubleshoot and improve key performance metrics such as average time to respond.

Easy to scale. An effective secure SD-WAN solution can also help organizations dynamically scale out to thousands of branches, seamlessly interoperate with existing physical and cloud infrastructures, and provide remote troubleshooting to eliminate costly physical interventions by skilled technicians.

SD-Branch, ZTNA, and SASE

An effective secure SD-WAN solution should also do more than just address the problems of the moment. It should also anticipate the networking and security needs of the near future as well, to provide flexibility, ensure consistency, and reduce total cost of ownership (TCO) over time. There are three specific capabilities that a solution should support for near-, medium-, and long-term distributed network needs.

Software-defined branch (SD-Branch). With enterprise branches directly accessing internet connections via SD-WAN, networking leaders need next-generation security while enabling multi-path WAN to improve application performance. Expanding on the capabilities of SD-WAN, secure SD-Branch capabilities offer protection for both wired and wireless connections, access controls, and the ability to see and monitor all devices connected to the branch network.[5] An effective secure SD-Branch deployment seamlessly integrates and manages networking and security capabilities across the WAN edge (local-area networking [LAN], wireless LAN, network access control, and wireless WAN).

Organizations need an SD-Branch solution that provides greater reach, flexibility, and adaptability without compromising on protection.[6]

Zero-trust network access (ZTNA). Organizations need predictable application performance across locations and an effective security posture. Today's "work-from-anywhere" paradigm requires explicit application access per user. Built-in ZTNA controls enhance both security and user experience by reducing risks while simplifying access—both off- and on-network. The core operating principle of ZTNA is that no user or device should ever be granted access to resources based solely upon location on the network.[7] Look for a secure SD-WAN solution that offers a built-in access proxy.

Secure access service edge (SASE). Organizations of all sizes are increasingly adopting different cloud-based services, migrating existing applications to the cloud, and developing new cloud-native applications. A SASE architecture combines SD-WAN with ZTNA and other services and functions to build a cloud-aware and cloud-based secure network.[8] This framework enables cloud-delivered security and unified management.

Moving to a SASE model both requires and enables a zero-trust approach to network security.[9]

A Unified Approach to Remote Networking Needs

Today's distributed networks need to unify operations across campus networks, branch networks, home offices, public clouds, and on-premises data centers. SD-WAN that integrates a full set of networking and security features can enable this kind of unified WAN transformation by delivering both performance and protection where it's needed—at the ever-expanding network edge.

First and foremost, an effective secure SD-WAN solution should provide consistent defenses without sacrificing performance for security (or vice versa). It should empower IT teams by simplifying their architecture, management, and ongoing operations at virtually any scale. And finally, secure SD-WAN should provide a platform that includes future-proofing features so that organizations can implement advanced architectural enhancements (e.g., SD-Branch, ZTNA, SASE) at their own pace.

[1] Kiran Desai, "The Rapid Rise Of SD-WAN As Digital Acceleration Takes Root," Forbes, September 3, 2021.

[2] Ibid.

[3] Nirav Shah, "The Challenges of Inspecting Encrypted Network Traffic," Fortinet, August 4, 2020.

[4] Brenda R. Sharton, "Ransomware Attacks Are Spiking. Is Your Company Prepared?," Harvard Business Review, May 20, 2021.

[5] Michael Xie, "Without Security, SD-Branch Is Just 'SD Risk'," Forbes, April 24, 2020.

[6] Ibid.

[7] Mike Chapple, "Why it's SASE and zero trust, not SASE vs. zero trust," TechTarget, December 15, 2020.

[8] Ibid.

[9] Ibid.

FORTINET®

www.fortinet.com

October 27, 2021 8:58 AM

1247417-0-0-EN